21

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,057	06/28/2001	Curtis E. Jutzi	42390P11869	9317

8791 7590 01/25/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/895,057	**Applicant(s)** JUTZI ET AL.
	Examiner Ellen C. Tran	**Art Unit** 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: amendment filed 21 November 2005, with an original application filed 28 June 2001.

2. Claims 1-30 are currently pending in this application. Claims 1, 7, 11, 17, and 21 are independent claims. Claims 1, 7, 11, 17, and 21 have been amended.

3. Amendments to the claims are accepted.

Response to Arguments

4. Applicant's arguments with respect to claims 1-30 have been considered but have not been found persuasive.

In response to applicant's argument beginning on page 17, "Independent claims 1, 11, and 21 have been amended to include a similar feature of: performing security authentication of a content driver by a content decryption component in order to verify and identity of the content driver as a secure content driver, wherein the content driver and the content decryption component are located within a kernel operating application space ... Yeung does not teach or suggest a content driver and a content decryption component located within a kernel application space". The Office does not agree, a 'kernel' is known in the art as software code at the core of a hardware device (i.e. processor, CPU, or player) the CPU_ID in Yeung is interpreted to be located at the kernel application space. Furthermore the CPU_ID is used at the application level in order to generate the decryption key (i.e. decryption component) used at the application level to view the streaming content.

The previous rejection has been modified to account for the amended claims along with another rejection 102(e) rejection using Okabe et al. US Patent No. 6,889,208.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

6. **Claims 1-30,** are rejected under 35 U.S.C. 102(e) as being anticipated by Yeung et al. U.S. Patent No. 6,668,246 (hereinafter '246).

As to independent claim 1, "A method comprising: performing security authentication of a content driver by a content decryption component in order to verify an identity of the content driver as a secure content driver, wherein the content driver and the content decryption component are located within a kernel application space" is taught in '246 col. 6, lines 9-19;

"receiving an encrypted content stream from the secure content driver" is shown in '246 col. 6, lines 33-51;

"performing integrity authentication of a run-time image of the secure content driver; and while integrity authentication of the secure content driver is verified, streaming decrypted content to the secure content driver to enable playback of the decrypted content to a user" is disclosed in '246 col. 7, lines 35-67.

As to dependent claim 2, **"wherein performing security authentication further comprises: locating authorization information of the secure content driver; decrypting the authorization information received from the secure content driver; authenticating an identity of the secure content driver based on the decrypted authorization information; and authenticating an identity of the secure content driver based on the decrypted authorization information"** is taught in '246 col. 7, lines 34-54.

As to dependent claim 3, **"wherein authenticating the identity further comprises: calculating a hash value of a static image of the secure content driver prior to loading the secure content driver into memory; selecting a stored digital signature of the static image; decrypting the stored digital signature to retrieve a pre-calculated hash value of the secure content driver; comparing the pre-calculated hash value with the calculated hash value; and when the calculated hash value matches the pre-calculated hash value of the secure content driver, notifying the secure content driver of successful security authentication"** is shown in '246 col. 3, line 64 through col. 4, line 13.

As to dependent claim 4, **"wherein performing security authentication further comprises: once security authentication of the content driver is established, determining a run-time at memory location of the secure content driver; and establishing a function entry point for receiving the stream of encrypted content from the secure content driver"** is disclosed in '246 col. 7, lines 8-21.

As to dependent claim 5, **"further comprising: receiving a content decryption key in order to enable decryption of encrypted content streams received from the secure content driver; receiving a digital signature of a static image of the secure content driver; and**

receiving a digital signature of a run-time image of the secure content driver" is taught in '246 col. 3, line 64 through col. 4, line 13.

As to dependent claim 6, **"wherein performing integrity authentication further comprises: decrypting the encrypted content stream received from the secure content driver; while decrypting the received encrypted content stream, performing a hash value calculation of code segments that perform functionality of the secure content driver while loaded in memory; selecting a stored digital signature of a run-time image of the secure content driver; decrypting the digital signature to reveal a run-time hash value; comparing the computed hash value with the run-time hash value of the secure content driver; and while the calculated hash value matches the run-time hash value of the secure content driver, repeating the decryption, the performing, the selecting and the comparing until decryption of the received encrypted content stream is complete"** is shown in '246 col. 3, line 41 through col. 4, line 21.

As to independent claim 7, **"A method comprising: establishing security authentication from a content decryption component, such that a content driver is verified as a secure content driver, wherein the content driver and the content decryption component are located within a kernel application space"** is taught in '246 col. 4, lines 15 through col. 5, line 2;

"when establishment of security authentication is successful, receiving access to a callback function in order to receive clear, decrypted content streams from the content decryption component; receiving a stream of encrypted content; streaming the encrypted content to the content decryption component; and when security authentication is

successfully established, receiving clear, decrypted content from the content decryption component via the received callback function" is disclosed in '246 col. 7 lines 8-67.

As to dependent claim 8, **"wherein establishing security verification further comprises: receiving a request for authorization information from the content decryption component; transmitting the requested authorization information to the content decryption component; and when security authentication is successfully established, receiving notification of successful security authentication from the content decryption component, such that the content driver is established as the secure content driver"** is shown in '246 col. 3, line 29 through col. 4, line 13.

As to dependent claim 9, **"wherein establishing security authentication further comprises: once security authentication is established, providing content decryption component with a memory location wherein the secure content driver is loaded at run-time; and providing the content decryption component with a function entry point for receiving the stream of encrypted content"** is disclosed in '246 col. 7, line 8-21.

As to dependent claim 10, **"wherein receiving encrypted content further comprises: receiving encrypted content from a content source reader; and receiving a direction from a content driver to stream the encrypted content to the content decryption component"** is taught in '246 col. 7, lines 35-43.

As to independent claim 11, this claim is directed to a computer readable medium of the method of claim 1; therefore it is rejected along similar rationale.

As dependent claims 12- 16, these claims contain substantially similar subject matter as claims 2-6; therefore they are rejected along similar rationale.

As to independent claim 17, this claim is directed to a computer readable medium of the method of claim 7; therefore it is rejected along similar rationale.

As dependent claims 18-20, these claims contain substantially similar subject matter as claims 8-10; therefore they are rejected along similar rationale.

As to independent claim 21, this claim is directed to the apparatus of the method of claim 1; therefore it is rejected along similar rationale.

As dependent claims 21-26, these claims contain substantially similar subject matter as claims 2-6; therefore they are rejected along similar rationale.

As dependent claims 27-30, these claims contain substantially similar subject matter as claims 7-10; therefore they are rejected along similar rationale.

7. **Claims 1-30,** are rejected under 35 U.S.C. 102(e) as being anticipated by Ishibashi US Patent No. 6,782,476 (hereinafter '476).

As to independent claim 1, "A method comprising: performing security authentication of a content driver by a content decryption component in order to verify an identity of the content driver as a secure content driver, wherein the content driver and the content decryption component are located within a kernel application space" is taught in '476 col. 4, lines 15 through col. 5, line 2;

"receiving an encrypted content stream from the secure content driver" is shown in '476 col. 5 lines 29-36;

"performing integrity authentication of a run-time image of the secure content driver; and while integrity authentication of the secure content driver is verified, streaming

decrypted content to the secure content driver to enable playback of the decrypted content to a user" is disclosed in '476 col. 6, lines 3-15.

As to dependent claim 2, **"wherein performing security authentication further comprises: locating authorization information of the secure content driver; decrypting the authorization information received from the secure content driver; authenticating an identity of the secure content driver based on the decrypted authorization information; and authenticating an identity of the secure content driver based on the decrypted authorization information"** is taught in '476 col. 4, lines 52-63.

As to dependent claim 3, **"wherein authenticating the identity further comprises: calculating a hash value of a static image of the secure content driver prior to loading the secure content driver into memory; selecting a stored digital signature of the static image; decrypting the stored digital signature to retrieve a pre-calculated hash value of the secure content driver; comparing the pre-calculated hash value with the calculated hash value; and when the calculated hash value matches the pre-calculated hash value of the secure content driver, notifying the secure content driver of successful security authentication"** is shown in '476 col. 5, lines 54-61.

As to dependent claim 4, **"wherein performing security authentication further comprises: once security authentication of the content driver is established, determining a run-time at memory location of the secure content driver; and establishing a function entry point for receiving the stream of encrypted content from the secure content driver"** is disclosed in '476 col. 7, lines 57 through col. 8, line 16.

As to dependent claim 5, "further comprising: receiving a content decryption key in order to enable decryption of encrypted content streams received from the secure content driver; receiving a digital signature of a static image of the secure content driver; and receiving a digital signature of a run-time image of the secure content driver" is taught in '476 col. 3, line 64 through col. 4, line 13.

As to dependent claim 6, "wherein performing integrity authentication further comprises: decrypting the encrypted content stream received from the secure content driver; while decrypting the received encrypted content stream, performing a hash value calculation of code segments that perform functionality of the secure content driver while loaded in memory; selecting a stored digital signature of a run-time image of the secure content driver; decrypting the digital signature to reveal a run-time hash value; comparing the computed hash value with the run-time hash value of the secure content driver; and while the calculated hash value matches the run-time hash value of the secure content driver, repeating the decryption, the performing, the selecting and the comparing until decryption of the received encrypted content stream is complete" is shown in '476 col. 6, lines 3-27.

As to independent claim 7, "A method comprising: establishing security authentication from a content decryption component, such that a content driver is verified as a secure content driver, wherein the content driver and the content decryption component are located within a kernel application space" is taught in '476 col. 4, lines 15 through col. 5, line 2;

"when establishment of security authentication is successful, receiving access to a callback function in order to receive clear, decrypted content streams from the content decryption component; receiving a stream of encrypted content; streaming the encrypted content to the content decryption component; and when security authentication is successfully established, receiving clear, decrypted content from the content decryption component via the received callback function" is disclosed in '476 col. 6, lines 3-15.

As to dependent claim 8, "wherein establishing security verification further comprises: receiving a request for authorization information from the content decryption component; transmitting the requested authorization information to the content decryption component; and when security authentication is successfully established, receiving notification of successful security authentication from the content decryption component, such that the content driver is established as the secure content driver" is shown in '476 col. 6, lines 45-67.

As to dependent claim 9, "wherein establishing security authentication further comprises: once security authentication is established, providing content decryption component with a memory location wherein the secure content driver is loaded at run-time; and providing the content decryption component with a function entry point for receiving the stream of encrypted content" is disclosed in '476 col. 6, lines 3-35.

As to dependent claim 10, "wherein receiving encrypted content further comprises: receiving encrypted content from a content source reader; and receiving a direction from a content driver to stream the encrypted content to the content decryption component" is taught in '476 col. 6, lines 3-15.

As to independent claim 11, this claim is directed to a computer readable medium of the method of claim 1; therefore it is rejected along similar rationale.

As dependent claims 12- 16, these claims contain substantially similar subject matter as claims 2-6; therefore they are rejected along similar rationale.

As to independent claim 17, this claim is directed to a computer readable medium of the method of claim 7; therefore it is rejected along similar rationale.

As dependent claims 18-20, these claims contain substantially similar subject matter as claims 8-10; therefore they are rejected along similar rationale.

As to independent claim 21, this claim is directed to the apparatus of the method of claim 1; therefore it is rejected along similar rationale.

As dependent claims 21-26, these claims contain substantially similar subject matter as claims 2-6; therefore they are rejected along similar rationale.

As dependent claims 27-30, these claims contain substantially similar subject matter as claims 7-10; therefore they are rejected along similar rationale.

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Sullivan et al	U.S. Patent No. 6,069,647	issued dated: May 30, 2000
Okabe et al.	U.S. Patent No. 6,889,208	issued dated: May 3, 2005

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen. Tran
Patent Examiner
Technology Center 2134
19 January 2006

Gilberto
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100